Abstract

Methods and apparatus are disclosed for generation of secure and efficient digital signatures in an information processing system. The system includes one or more user devices, a signing aid or other intermediary device, and a verifier. A given user device has associated therewith key pairs (s, p) and (s', p') corresponding to respective first and second digital signature protocols. As part of a setup process, an agreement relating to the public keys p and p' is signed by both the user device and the intermediary device, and the resulting twice-signed agreement is stored by both the user device and the intermediary device. A first digital signature $s1$ is then generated on a message m or a hash $h(m)$ thereof in the user device using the secret key s' and is sent to the verifier. The verifier in turn sends $s1$ to the intermediary, and the intermediary checks that $s1$ is a valid digital signature for the user device. If $s1$ is valid, the intermediary device generates a second digital signature $s2$ on m or $h(m)$ using the secret key s, and $s2$ is returned to the verifier as a signature generated by the user device. The intermediary may be configured to wait a predetermined delay period between checking that $s1$ is a valid signature and generating $s2$, such that a user may contact the intermediary device and upon providing an access code thereto direct the intermediary device not to generate $s2$.